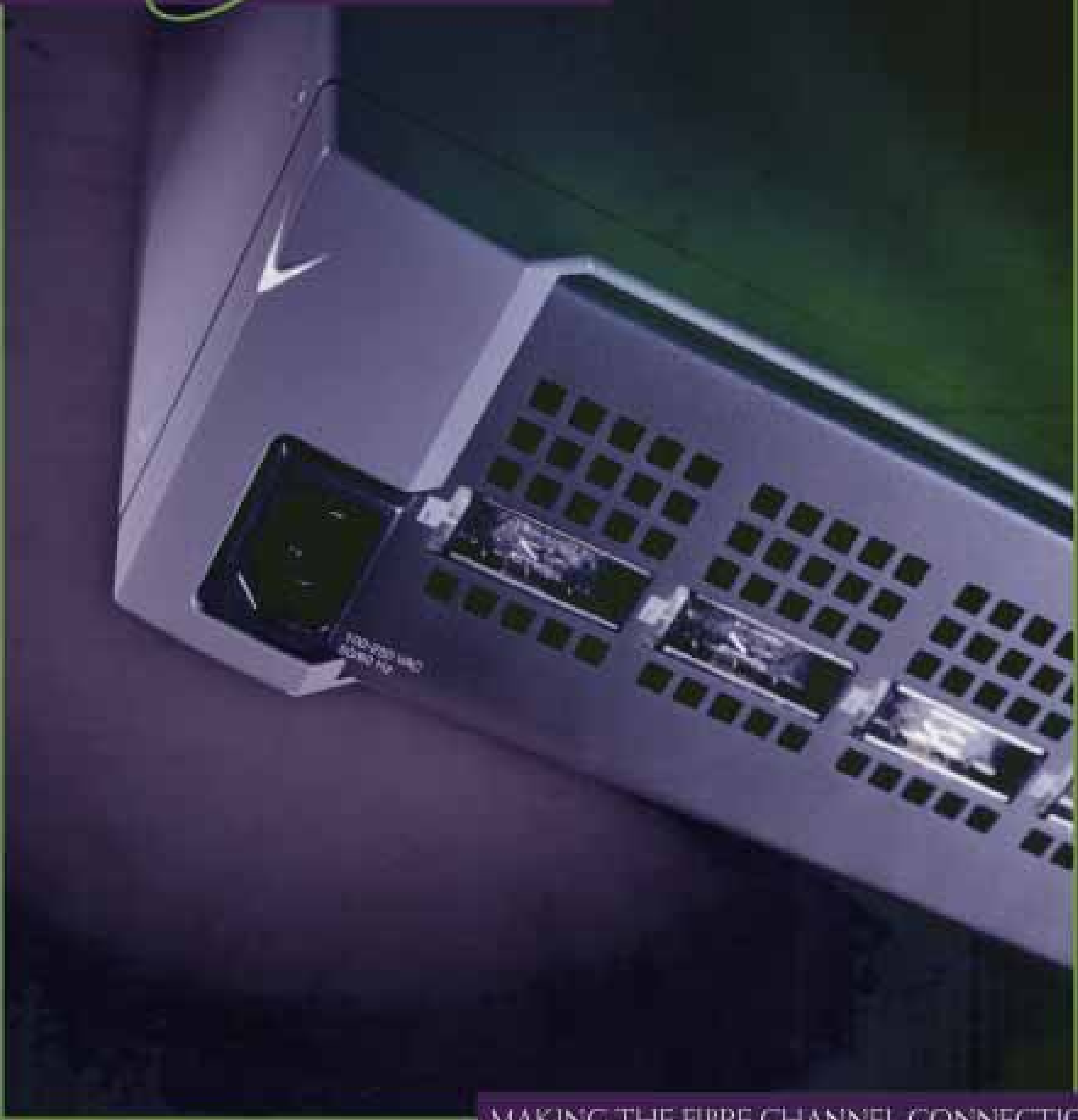
VIXEL



MAKING THE FIBRE CHANNEL CONNECTION

Vixel 8100 Installation & Troubleshooting Guide

Copyright © 2001 Vixel Corporation. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Vixel Corporation.

Information furnished by Vixel Corporation is believed to be accurate and reliable. However, no responsibility is assumed by Vixel Corporation for its use; or for any infringements of patents of other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Vixel Corporation.

Vixel is a registered trademark of Vixel Corporation. SAN InSite is a trademark of Vixel Corporation. All other brand or product names referenced herein are trademarks or registered trademarks of their respective companies or organizations.

Vixel Corporation provides this manual “as is,” without any warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Vixel Corporation may make improvements and changes to the product described in this manual at any time and without any notice. Vixel Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties that may result. Periodic changes are made to information contained herein; although these changes will be incorporated into new editions of this manual, Vixel Corporation disclaims any undertaking to give notice of such changes.

Vixel Corporation, 11911 North Creek Parkway South, Bothell, WA 98011

Table of Contents

1 Introduction 1
  Features 1
  Description 2

2 Unpacking and Installing the Vixel 8100 7
  Unpacking 7
  Installing (Rack-Mounting and GBIC Insertion) 8

3 Interfacing to the Switch 15
  Using the 8100 IP Utility (Ethernet or SLIP) 16
  Using Workstation IP Configuration (Ethernet) 18
  Using SLIP and Dial-Up 19

4 Theory of Operation 25
  Fabric Mode Operation 25
  Stealth Mode Operation 26

5 Troubleshooting 36
  Understanding Start-up (POST) LED Sequence 36
  Running POST Diagnostics 38
  Answers to Common Questions 40

6 Technical Reference 42
  Default Switch Settings 42
  Technical Support 45
  Fibre Channel References 45

A Event Messages 46

B Glossary 57

Index 60

CHAPTER 1 Introduction

Features 1

Description 2

Important safety, electromagnetic compatibility, and regulatory information is contained in the guide titled *Vixel Safety & Regulatory Guide*. The installation and use of this product must be in accordance with the information given in that guide.

The Vixel 8100 provides complete Fibre Channel fabric support, true line-speed switching, and the flexibility of GBIC-based design. Private loop and fabric devices are supported.

Private loop devices are supported through Vixel's stealth mode, which allows non-fabric ready devices to attach to and benefit from the dedicated bandwidth of the Vixel 8100. Even though private loop devices do not support Simple Name Server (SNS) or Fabric Login, the Vixel 8100 stealth mode allows you to segment and interconnect these devices into multiple loops, allowing each pair of ports to use 100Mbyte bandwidth. Stealth mode's non-blocking architecture provides increased performance over the current non-switched topologies.

Fabric devices are supported through fabric mode using Simple Name Server (SNS) and Fabric Login.

Features

The Vixel 8100 has several features:

- Eight media interface ports for GBICs.
- Several system and port LED indicators, including power and fault.
- A management interface—SAN InSite—that allows you to configure and monitor switch ports via Ethernet or RS-232.
- Zoning to allow groups on one fabric topology to keep their data separate.
- Aggregate bandwidth of 16 Gbps per unit.
- Fully non-blocking architecture.
- Buffering for up to 32 maximum size frames per port.
- Hardware-implemented routing with a route determination time less than two micro-seconds.
- Redundant fans for high availability.

- An auto-sensing power-supply that supports 100VAC through 250VAC, 50 or 60 Hz.

Description

Power Supply and Ethernet Port

The universal power supply is an auto ranging supply that senses both the frequency (50 or 60 Hz) and input voltage for voltages between 100VAC through 250VAC. The Ethernet port is 10BaseT.

Environmental Requirements

The Vixel 8100 must be operated in a clean and dry environment with unrestricted airflow. Maintain three to four inches of clearance on both ends (GBIC and logo ends) and avoid overheating—do not place the Vixel 8100 on heat-generating surfaces. Operating conditions follow.

Requirement	Value
Operation	0°C to 50°C normal operation (ambient temperature)
Storage	-40°C to 75°C non-condensing
Power	100VAC to 250VAC; 60 Hz for domestic, 50 or 60 Hz for international; 1.0 A maximum

Ports and LEDs

The Vixel 8100 is equipped with eight Fibre Channel ports. Port and system LEDs are shown below.

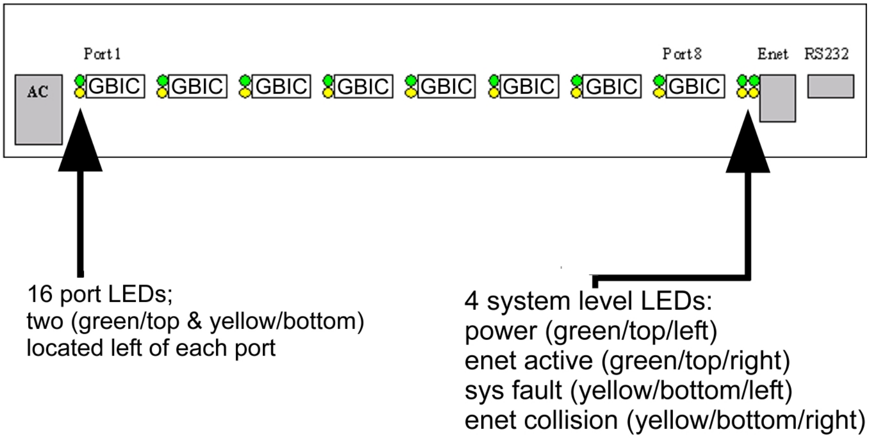

Port1
Port8
Enet
RS232
AC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
16 port LEDs;
two (green/top & yellow/bottom)
located left of each port
4 system level LEDs:
power (green/top/left)
enet active (green/top/right)
sys fault (yellow/bottom/left)
enet collision (yellow/bottom/right)

Figure 1-1

LED indications during operation are shown in the tables below.

Power LED (green)	Indication during Operation
Off	Power is off.
Solid	Power is on.
Blink	A power problem has occurred.

System LED (yellow)	Indication during Operation
Off	Normal operation (no system errors).
Blink (slow)	A system error has occurred.
Blink (fast)	A system critical error has occurred; for example, a fan is not operating.

Enet Active LED (green)	Indication during Operation
Off	Ethernet not present.
Solid	Ethernet is present but not active.
Random Flicker (rate depends on amount of traffic)	Ethernet is present and active (transmitting packets).

Enet Collision LED (yellow)	Indication during Operation
Off	No ethernet collisions are occurring.
Flicker (may occur during heavy traffic)	A collision is occurring during a packet transmission.

Green Port LED	Yellow Port LED	Indication during Operation
Off	Off	GBIC not inserted.
Off	Solid	GBIC inserted but bad. Possible transmitter fault.
Solid	Off	GBIC inserted and good; link is established.
Solid	Solid	GBIC inserted and good, but no link is established.
Solid	Blink	Port has been forced off-line (busy-out)
Blink	Blink	Port is being “beaconed” by a management entity (such as SAN InSite).

GigaBit Interface Converters (GBICs)

The Vixel 8100 ports are compliant with the GigaBit Interface Converter (GBIC) Specification. The currently available GBIC media types are full-speed (1.0625 Gigabits per second or Gbaud). The three GBIC media types follow:

- Short-Wave Optical GBIC (OE1063SW)
  - Uses dual SC fiber optic connectors
  - Supports multimode 50 µm fiber – 2 meters/minimum, 500 meters/maximum
  - Supports multimode 62.5 µm fiber – 2 meters/minimum, 350 meters/maximum
  - Wavelength – 790nm (typical, range between 770-860nm)
  - Non-OFC laser
  - Compliant with Fibre Channel FC-PH-2 physical layer option 100-M5-SN-I
- Copper GBIC
  - Uses AMP™ HSSDC (FC-PH-3 Style II) or DB-9 (Passive or Active) connector
  - Intra-cabinet maximum length is 13 meters
  - Inter-cabinet maximum length is 33 meters
  - For lengths over 25 meters, use equalized cables (these cables contain special circuitry that prevents high-frequency loss and general signal degradation)
- Long-Wave Optical GBIC (OE1063LW)
  - Uses dual SC fiber optic connectors
  - Uses single-mode 9 µm fiber
  - Fiber lengths – 2 meters/minimum, 10 kilometers/maximum
  - Wavelength – 1310nm (range between 1280-1330nm)
  - Non-OFC laser

CHAPTER 2

Unpacking and Installing the Vixel 8100

Unpacking 7

Installing (Rack-Mounting and GBIC Insertion) 8

Important safety, electromagnetic compatibility, and regulatory information is contained in the guide titled *Vixel Safety & Regulatory Guide*. The installation and use of this product must be in accordance with the information given in that guide.

Unpacking

To unpack the Vixel 8100:

1. Save the shipping container, foam, and anti-static bags—returning the Vixel 8100 in any other container or packing material may void its warranty.
2. Inspect the unit thoroughly and immediately report any signs of damage to your sales representative and to the shipping agency.

3. Ensure that you have received the following items:
   - Vixel 8100 unit, packed in foam and an anti-static bag
   - Vixel 8100 Media Kit:
     - This Installation and Troubleshooting Guide
     - SAN InSite CD, Quick Reference Card, and New Features and Release Notes
     - Configuration sheet specifying the Vixel 8100's as-shipped configuration (which should reflect your site's stated requirements)
     - In Europe, a Declaration of Conformity
     - Four (4) rubber feet
   - Power cord (standard, with a U.S.-type power cord; NEMA styles)
   - Rack Mount Kit (optional) with the following components:

Component	Quantity
Support slides	2
Mounting ears	2
Bracket extensions	2
Nutplates (rack)	6
Nutplates (extender)	2
10-32 pan head screws	16
10-32 flat head screws (for extender-to-slide connection)	8
Washers	12

Installing (Rack-Mounting and GBIC Insertion)

Before you rack mount the Vixel 8100 and/or insert GBICs, obtain the following items:

Note: For instructions on installing the SAN InSite software, see the SAN InSite quick reference card or the documentation included on the SAN InSite CD.

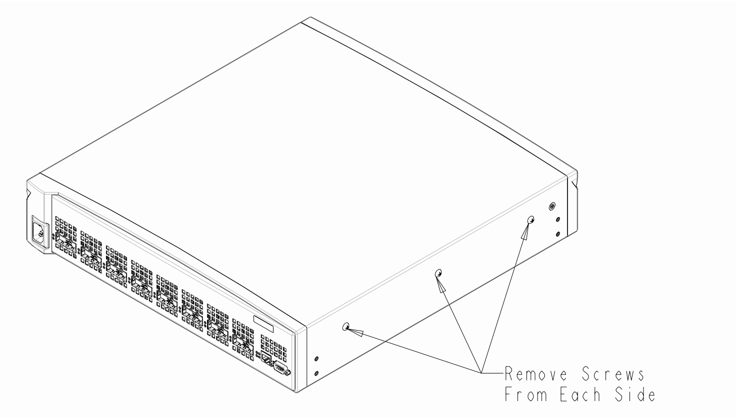
- Serial DB-9 null-modem cable.
- Cables that are appropriate to the cabling layout of your site. (If needed, contact Vixel Corporation for a list of vendors qualified to sell cables built for Fibre Channel equipment.)
- *If rack mounting is needed,* the optional Rack Mount Kit option shipped with the Vixel 8100.

Rack Mounting the Vixel 8100

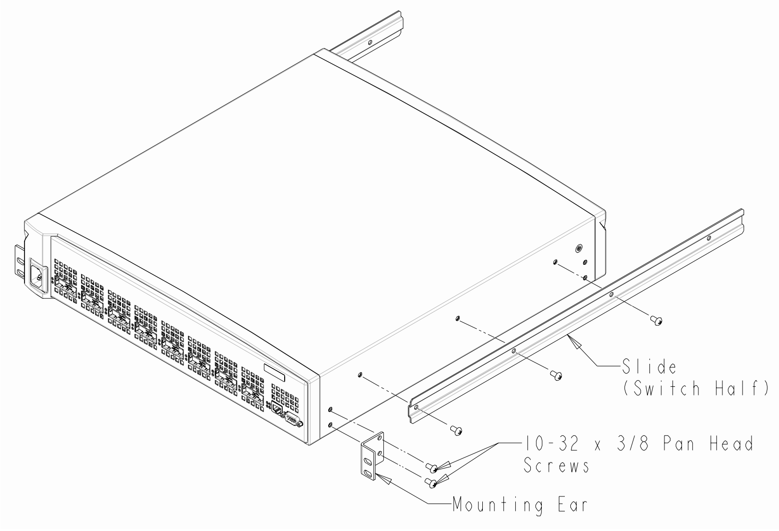
To mount the Vixel 8100 in a standard, 19" rack:

Note: The Vixel 8100 can be mounted with either the GBIC or logo side out of the rack. (The power plug is on the GBIC side of the Vixel 8100.)

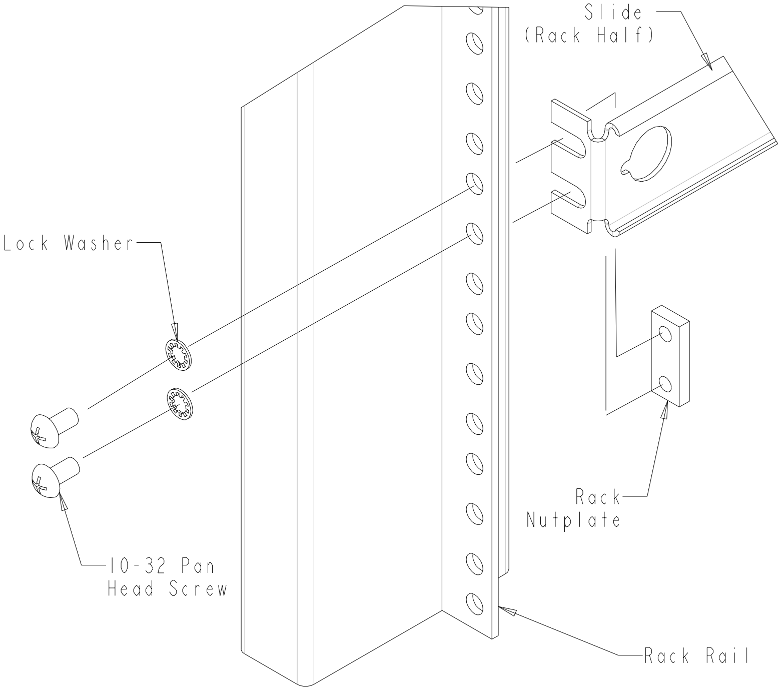
1. Decide which panel of the switch you want at the end of the rack.
2. For each side of the Vixel 8100 switch:
   a. Remove the three (3) top screws



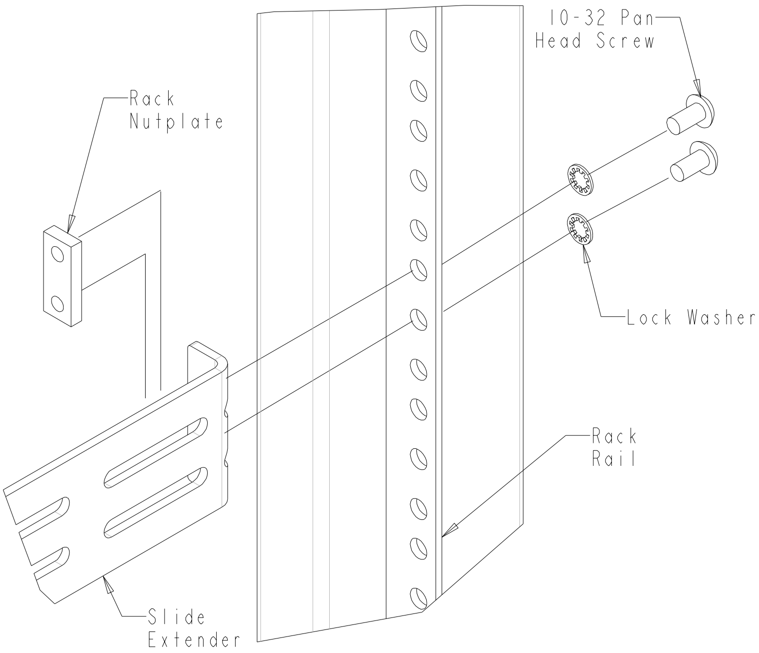
   b. Attach a support slide (switch part) to the switch using the three (3) top screws, according to the decision made in step 1.
   c. Attach mounting ear.



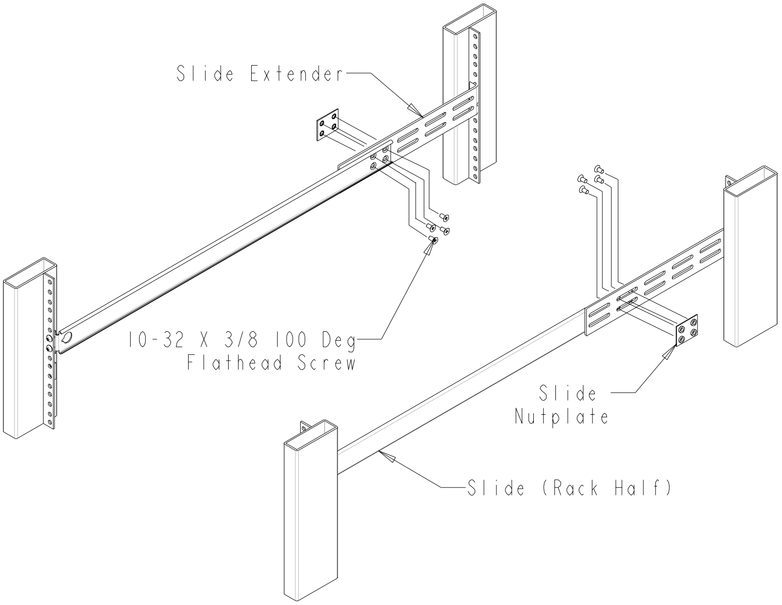
3. Install slide (rack half) to the rack rails. Do not tighten the fasteners that attach slide to rack rails yet.



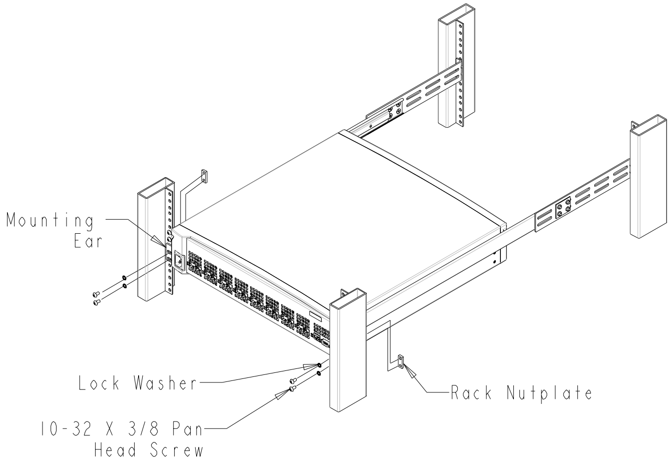
4. Attach slide extender to the rack rail.



5. Fasten slide extender to the slide.



6. Slide the Vixel 8100 onto the rack and install screws, washers, and nutplates to lock ears to rails of rack.



7. Tighten the screws that attach the bracket extension/support slide (rack part).
8. Attach one end of the Vixel 8100 power cord to the power inlet socket located in the GBIC side of the Vixel 8100 chassis and the other end to a properly earthed receptacle (outlet).

   The Vixel 8100 is now rack-mounted and turned on. At start-up, the Vixel 8100 follows the Power-On Self-Test (POST) sequence.

Note: The plug on the power cord is intended to serve as the disconnect device.

Start-up (POST)

The Vixel 8100 runs through Power On Self Test (POST) diagnostics to verify the fundamental integrity of the Vixel 8100 box, port memory (flash and SDRAM), and related circuitry. The POST sequence follows.

1. All LEDs turn solid for one second.
2. In sequence from left to right, each green port LED turns solid during a major POST test. (Length of time varies for each test.)
3. *If (a) all green port LEDs have turned solid then off and (b) all LEDs then turn off,* the Vixel 8100 has passed all POST tests and is ready for operation.
   If a yellow port LED blinks, the Vixel 8100 has failed a POST test.
   See“Running POST Diagnostics” on page 38 to run POST diagnostics and find the numbers of the failed test, subtest, and error code.

Inserting and Removing GBICs

The Vixel 8100 ports are compliant with the GigaBit Interface Converter (GBIC) Specification.

Note: For optical GBIC ports, remove the factory-installed dust covers or plugs before GBIC insertion.

To insert a Gigabit Interface Converter (GBIC) into a Vixel 8100 port, use minimal pressure, fitting the GBIC housing's integral guide key into the port until the GBIC's tabs click into place. Cables can be attached to GBICs before or after GBIC insertion; ports with installed GBICs but without attached cables are bypassed.

WARNING: GBICs emit invisible laser radiation. Do not stare into the transmitted beam.

CAUTION: Forcing a GBIC into a port may damage the GBIC and/or port.

CAUTION: Do not bend fiber-optic cables more than the bend radius specified by the cable manufacturer.

To remove a GBIC from a Vixel 8100 port, simultaneously press the tabs on each side inward while slowly removing the GBIC. Cables can be removed from the GBICs before or after GBIC removal; ports with installed GBICs but without attached cables are bypassed.

The currently available GBIC media types are full-speed (1.0625 Gigabits per second or Gbaud). The three GBIC media types follow:

- Short-Wave Optical GBIC (OE1063SW)
  - Uses dual SC fiber optic connectors
  - Supports multimode 50 µm fiber – 2 meters/minimum, 500 meters/maximum
  - Supports multimode 62.5 µm fiber – 2 meters/minimum, 175 meters/maximum
  - Wavelength – 790nm (typical, range between 770-860nm)
  - Non-OFC laser
  - Compliant with Fibre Channel FC-PH-2 physical layer option 100-M5-SN-I
- Copper GBIC
  - Uses AMP HSSDC (FC-PH-3 Style II) or DB-9 (Passive or Active) connector
  - Intra-cabinet maximum length is 13 meters
  - Inter-cabinet maximum length is 33 meters
  - For lengths over 25 meters, use equalized cables (these cables contain special circuitry that prevents high-frequency loss and general signal degradation)

- Long-Wave Optical GBIC (OE1063LW)
    - Uses dual SC fiber optic connectors
    - Uses single-mode 9 µm fiber
    - Fiber lengths – 2 meters/minimum, 10 kilometers/maximum
    - Wavelength – 1310nm (range between 1280-1330nm)
    - Non-OFC laser

CHAPTER 3 Interfacing to the Switch

Using the 8100 IP Utility (Ethernet or SLIP) 16
Using Workstation IP Configuration (Ethernet) 18
Using SLIP and Dial-Up 19

Note: To configure and monitor the Vixel 8100 after connection, see the SAN InSite documentation.

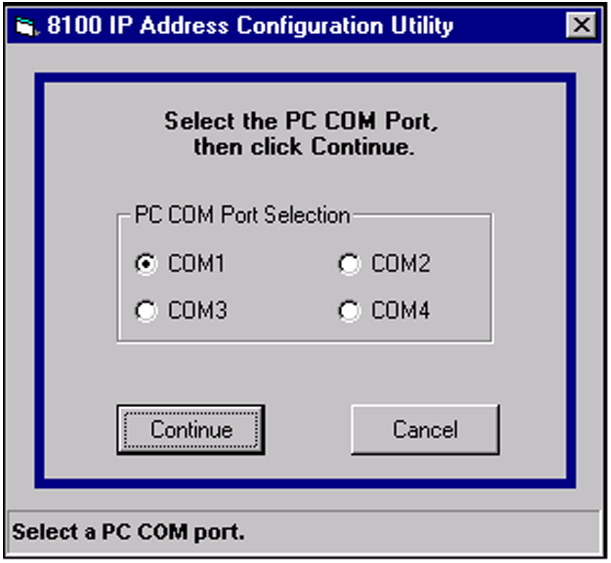
You can interface to the Vixel 8100 through any of the following methods: 8100 IP Utility, configuring the workstation (Ethernet), or SLIP and Dial-Up. Requirements and time needed for each method follow.

Connection Method	Requirements	Estimated Time Needed
8100 IP Utility (Ethernet or SLIP)	• installed 8100 IP Utility (from SAN InSite CD) • Windows NT® platform • serial cable	1-2 minutes
Workstation IP Configuration (Ethernet)	• installed SAN InSite application • EITHER ethernet cable and ethernet hub OR ethernet crossover cable	5-10 minutes
SLIP and Dial-Up	• serial cable • Dial-Up Networking (see instructions on page 20)	30 minutes (including initial set-up)

Using the 8100 IP Utility (Ethernet or SLIP)

Note: The 8100 IP Utility is automatically installed along with SAN InSite.

1. From the Start menu, choose **Programs**, then **Vixel**, then **8100 IP Utility**. The 8100 IP Address Configuration Utility dialog box appears.



8100 IP Address Configuration Utility

Select the PC COM Port, then click Continue.

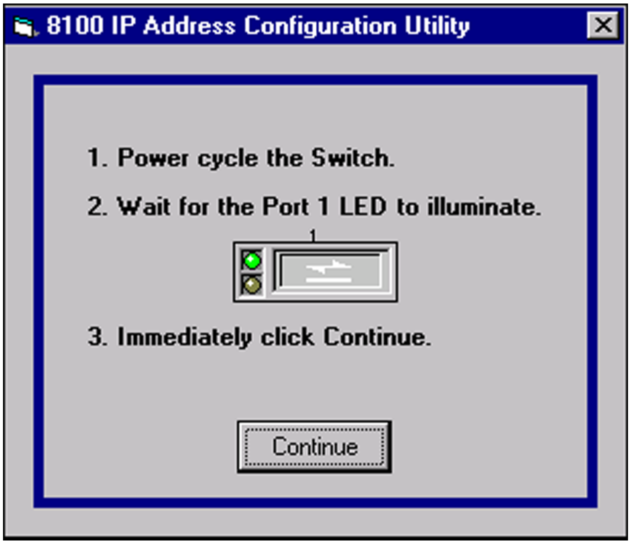
PC COM Port Selection

● COM1 ○ COM2

○ COM3 ○ COM4

Select a PC COM port.

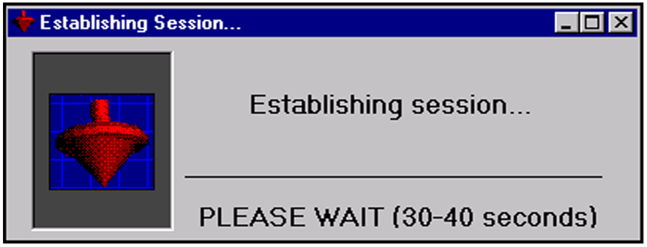
2. Select the desired COM port (usually COM1) and click **OK**. The dialog box displays a “Power cycle...” message.



8100 IP Address Configuration Utility

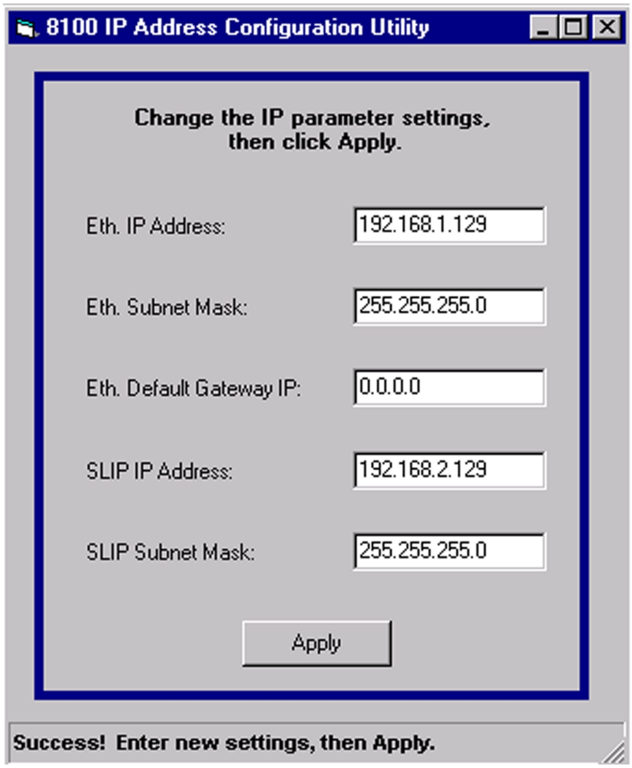
1. Power cycle the Switch.
2. Wait for the Port 1 LED to illuminate.
3. Immediately click Continue.

3. Power cycle the switch; while the Port 1 LED is illuminated, click **Continue.**
   The “Establishing Session...” message appears briefly, then the 8100 IP Address Configuration Utility reappears, displaying the active (default) settings.



Establishing session...

PLEASE WAIT (30-40 seconds)



Change the IP parameter settings, then click Apply.

Eth. IP Address: 192.168.1.129
Eth. Subnet Mask: 255.255.255.0
Eth. Default Gateway IP: 0.0.0.0
SLIP IP Address: 192.168.2.129
SLIP Subnet Mask: 255.255.255.0

Success! Enter new settings, then Apply.

4. Type the desired IP parameters (Ethernet and/or SLIP) and click **Apply.**
   The “Validating IP settings...” message appears in the status bar at the bottom of the dialog box.
5. In the resulting “Verification successful!” message box, click **OK.**
6. Power cycle the switch; close the utility if desired.
   The IP parameters are now changed.

Using Workstation IP Configuration (Ethernet)

The Vixel 8100's default IP address for the Ethernet port is 192.168.1.129.

Note: These instructions assume a Windows NT PC operating system. Modify these instructions as needed for your operating system.

First, configure the workstation's IP address (for the same subnet):

1. Double-click **My Computer**, then **Control Panel**, then **Network.**
2. In the resulting Network dialog box, click the **Protocols** tab.
3. In the resulting Protocols tab, double-click **TCP/IP Protocol**.
4. In the resulting TCP/IP Protocol dialog box (IP Address tab), ensure that "Specify an IP address" is selected.
5. Note the IP address.
6. In the IP Address textbox, type **192.168.1.XXX** (where **XXX** is any one-, two-, or three-digit number other than the default "129").
7. Click **Apply**, then click **OK** twice.
8. If your workstation requires a reboot to activate changes, then reboot.

Second, configure the switch's IP address (for the same subnet):

1. *For an ethernet network connection,* attach the RJ45 end of an ethernet cable to an ethernet port on the Vixel 8100 and the other end to a port on an ethernet hub.
   For a direct ethernet connection, attach the RJ45 end of an ethernet crossover cable to an ethernet port on the Vixel 8100 and the other end to a workstation.
2. In SAN InSite, add the switch under its default ethernet IP address (192.168.1.129), then change the switch's IP address, subnet mask, and default gateway as desired. (For instructions on changing switch IP parameters in SAN InSite, see the SAN InSite documentation.)
3. Remove the switch entry from SAN InSite. (The switch needs to be added later under its new IP address.)

Note: If the switch is not detected under its default ethernet IP address, see CHAPTER 5 on page 36 for troubleshooting information.

Third, reset the workstation's IP address:

1. Repeat configuration of the workstation's IP address to attain the original address (noted in "First," step 5).
2. If your workstation requires a reboot to activate changes, then reboot.
3. Reboot the switch (power off, then power back on).

   You can now add the switch under its new IP address and configure and monitor through SAN InSite. (For instructions, see the SAN InSite documentation.)

Using SLIP and Dial-Up

The SLIP and Dial-Up method allows you to later manage the switch through SLIP instead of Ethernet, if desired. The Vixel 8100's default IP address for the SLIP port is 192.168.2.129.

Note: These instructions assume a Windows NT PC operating system. Modify these instructions as needed for your operating system.

To connect through SLIP:

1. Ensure that the items listed below have been correctly configured on the workstation (see "Correct Workstation Configurations for SLIP Connection" on page 20):
   - Dial-Up Networking and Modem
   - the Vixel 8100 phonebook entry
   - Remote Access Service
   - Dial-Up Adaptor
   - TCP/IP Protocol
2. Using a DB-9 null-modem serial cable, connect the MGMT-RS-232 port of the Vixel 8100 to a serial communication port (which is running the SLIP protocol) on the host workstation.
3. Note the workstation port that is being used.
4. Double-click **My Computer**, then double-click **Dial-Up Networking**.
5. In the resulting Dial-Up Networking window, select the Vixel 8100 phonebook entry in the "Phonebook entry to dial:" field and click **Dial**.

Note: Do not add a password.

6. In the resulting Connect to Vixel 8100 window, click **OK**.
7. *If an error message appears,* double-check your cabling connections and redial. If Windows hangs (because of the way NT handles serial port configuration), you might have to backtrack and manually hang up the connection, then redial.

   If the Connection Complete window appears, click **OK**.

   You now have a SLIP connection to the Vixel 8100. You can now add the switch under its new IP address and configure and monitor through SAN InSite. (For instructions, see the SAN InSite documentation.)

Correct Workstation Configurations for SLIP Connection

This section includes the following instructions:

- Installing dial-up networking and configuring a modem.
- Adding and configuring a Vixel 8100 phonebook entry.
- Ensuring correct configuration.

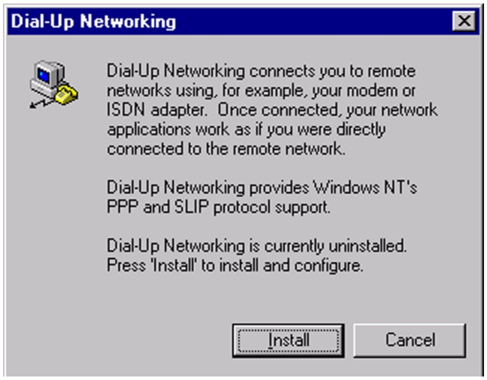
To install Dial-Up Networking and configure a modem:

1. Insert the Windows NT installation CD into the workstation's CD-ROM drive (or find network location).

Note: If Windows NT install/upgrade messages appear (from the CD), exit the messages and continue these instructions.

2. Double-click **My Computer**, then double-click **Dial-Up Networking**.

   The following message appears (if this message doesn't appear, Dial-Up Networking may not be installed).



Dial-Up Networking connects you to remote networks using, for example, your modem or ISDN adapter. Once connected, your network applications work as if you were directly connected to the remote network.

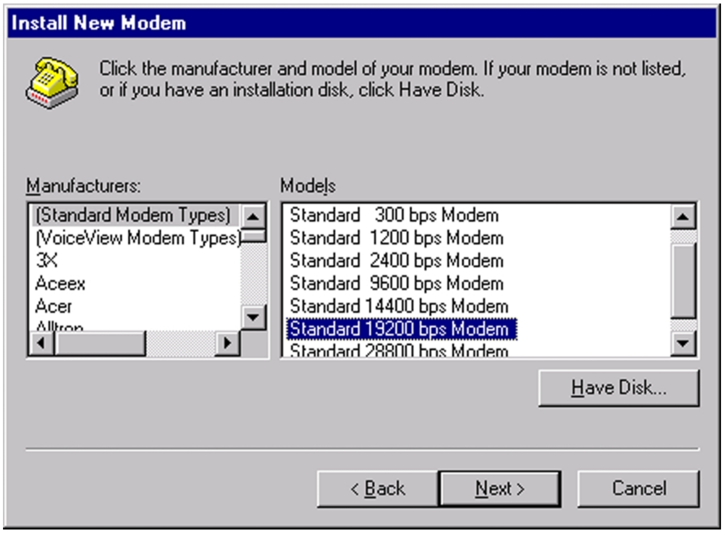
Dial-Up Networking provides Windows NT's PPP and SLIP protocol support.

Dial-Up Networking is currently uninstalled. Press 'Install' to install and configure.

3. Click **Install.**
4. *If Windows NT prompts for the location of the installation media,* specify the location and click OK. (Exit the NT install/upgrade screen if necessary.)

   Windows NT copies the necessary files, then searches for RAS-capable devices.
5. *If the "Do you want to add a modem..." message window appears,* click **Yes.**
6. In the resulting Install New Modem dialog box, click "Don't detect my modem; I will select it from a list" and click **Next.**

7. In the resulting dialog box, select (**Standard Modem Types**), then **Standard 19200 bps Modem,** and click **Next.**



Click the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.

Manufacturers:

(Standard Modem Types)
(VoiceView Modem Types)
3X
Aceex
Acer
Alltron

Models

Standard 300 bps Modem
Standard 1200 bps Modem
Standard 2400 bps Modem
Standard 9600 bps Modem
Standard 14400 bps Modem
Standard 19200 bps Modem
Standard 28800 bps Modem

8. In the resulting dialog box, select the COM port in which you have installed the SLIP management cable and click Next.
9. Click **Finish** in the “You have completed modem installation successfully...” message box, then click **OK** in the Add RAS Device window.
10. In the resulting Remote Access Setup window:
    a. Click Configure; ensure that **Dial Out Only** is selected and click **OK.**
    b. Click Network; ensure that **TCP/IP** is selected and click **OK.**
    c. Click **Continue.**

    A message appears stating that Dial-Up Networking was successfully installed and prompting you to restart the computer.

Note: If you are using an installation CD, remove it before clicking **Restart.**

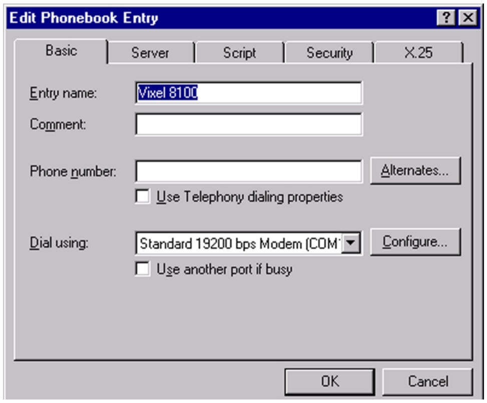
11. Click **Restart.**
12. After restart, double-click My Computer, then Control Panel, then Modems.
13. In the resulting Modems Properties window, select (**Standard 19200 bps Modem, ComX**) and click **Properties**:
    a. In the General tab, ensure that the Maximum speed is set to **19200.**
    b. In the Connection tab, ensure the following settings:
        - Data bits is set to 8.
        - Parity is set to None.
        - Stop bits is set to 1.
        - "No Call preferences" boxes (if available) are checked.
    c. Click **Advanced.**
14. In the Advanced Connection Settings dialog box, ensure that no checkboxes are checked and that the Extra settings field is blank.
15. Click **OK** twice; in the resulting Modems Properties dialog box, click Close.

To add and configure a phonebook entry for the Vixel 8100:

1. Double-click **My Computer**, then double-click **Dial-Up Networking**.
2. *If prompted for the local telephone area code,* type the correct area code and click **Continue**.
3. *If no entries exist,* click **OK** at the "The phonebook is empty..." message.

   If entries exist, but you need to add an entry for the Vixel 8100, click **New**.
4. In the resulting New Phonebook Entry Wizard dialog box:
   a. Type **Vixel 8100** in the "Name the new phonebook entry:" textbox and click **Next**.
   b. In the resulting Server dialog box, ensure that only the "The non-Windows NT server..." checkbox is checked and click **Next**.
   c. In the resulting Phone Number dialog box, leave all fields empty and click **Next**.
   d. In the resulting Serial Line Protocol dialog box, ensure that **SLIP** is selected and click **Next**.
   e. In the resulting Login Script dialog box, ensure that **None** is selected and click **Next**.
   f. In the My IP address textbox in the resulting IP Address dialog box, type **192.168.2.2** (or another IP address—192.168.2.XXX—in the same subnet as the default Vixel 8100 SLIP IP address of 192.168.2.129) and click **Next.**
   g. In the resulting Name Server Addresses dialog box, leave the fields empty and click **Next**.
   h. In the resulting New Phonebook Entry Wizard dialog box, click **Finish**.
5. In the resulting Dial-Up Networking dialog box, select **Vixel 8100**; from the More pull-down menu, select **Edit entry and modem properties**.

6. In the resulting Edit Phonebook Entry dialog box:
   a. In the Basic tab, ensure that the Vixel 8100 entry and the Standard 19200 bps Modem (COMX) selection are visible, that no checkboxes are checked, and that no fields contain values, as shown below.



Entry name: Vixel 8100
Comment:
Phone number:
☐ Use Telephony dialing properties
Dial using: Standard 19200 bps Modem (COM'
☐ Use another port if busy

   b. Click **Configure**.
   c. In the resulting Modem Configuration dialog box, ensure the settings below, then click **OK**.
      - Initial speed (bps) is set to **19200**.
      - Hardware Features checkboxes are not checked.
      - Disable modem speaker checkbox is checked.
   d. In the Server tab, ensure that the following settings are used.
      - **SLIP: Internet** is the selected Dial-up server type.
      - **TCP/IP** checkbox is checked.
      - All other fields are grayed out (not selectable).
   e. Click **TCP/IP Settings**.
   f. In the resulting SLIP TCP/IP Settings dialog box, ensure that the following settings are used, then click **OK**.
      - IP address is correct.
      - Name server addresses are not set.
      - Force IP header compression check box is not checked.
      - Frame size is set to **1500**.
   g. In the Script tab, ensure that **None** is selected for After dialing (login) and click **Before Dialing**.
   h. In the resulting Before Dialing Script dialog box, ensure that None is selected and click **OK.**
   i. In the Security tab, ensure that **Accept any authentication including clear text** is selected.
   j. In the X.25 tab, ensure that the following settings are used, then click **OK**.
      - **None** is selected for Network.
      - Other fields contain no values.
7. In the resulting Dial-Up Networking dialog box, click **Close**.

   The Vixel 8100 phonebook entry is now added and configured.

To ensure correct configuration of Remote Access Service, Dial-Up Adaptor, and TCP/IP Protocol:

1. Double-click Control Panel, then double-click Network.
2. In the Services tab of the resulting Network window, select **Remote Access Service** and click **Properties**.
3. In the resulting Remote Access Setup window, select Standard 19200 bps Modem, then:
   a. Click Configure and ensure that **Dial out only** is selected.
   b. Click Network and ensure that the **TCP/IP** checkbox is checked.
   c. Click **Continue**.
4. In the Bindings tab of the Network window:
   a. Click the plus sign (+) next to Remote Access Server Service, then click the plus sign (+) next to WINS Client; ensure that Remote Access WAN Wrapper is displayed.
   b. Click **OK.**
   c. Restart the workstation.

   The correct configuration of Remote Access Service, Dial-Up Adaptor, and TCP/IP Protocol is now ensured.

CHAPTER 4

Theory of Operation

Fabric Mode Operation 25

Stealth Mode Operation 26

Note: The Vixel 8100 is in stealth mode when it is shipped.

The Vixel 8100 has two operating modes: fabric and stealth. While private devices can connect to the Vixel 8100 under stealth mode only, public devices can connect under stealth or fabric mode. To choose between stealth and fabric modes, consider their operation (see sections below). Fabric mode's key advantage is its support for large and complex configurations while stealth mode can be used for simple configurations with less than 119 nodes. Each portion of the 24-bit Fibre Channel standard address—Domain, Area, and Port—functions differently depending on the operating mode.

Fabric Mode Operation

Addressing

In fabric mode, the Domain portion of the 24-bit Fibre Channel standard address represents the switch and the Area portion represents the port. For loop-specific addresses, the Port portion represents a particular AL_PA on the loop. (AL_PAs are assigned following ANSI standards.) While the Area and Port portions of the address are set automatically, the Domain portion is set through SAN InSite, as a hex value between 1 and EF. (Ask your network administrator for the desired unique domain for each switch.)

The frames sent by devices each carry a 24-bit destination address (D_ID) and a 24-bit source address (S_ID) in the frame header.

Port Types

Fabric mode supports three port types: F_Port, for point-to-point connections; FL_Port, for connections to loop protocol devices; and E_Port, for switch-to-switch connections.

Zoning

Note: When changing from stealth to fabric mode, SAN InSite disables zoning locally. Ensure desired zoning before writing to flash.

Both fabric and stealth modes support port zoning, which allows groups that share a fabric topology to keep their data separate. For example, human resources may not want other departments to be able to access sensitive data on devices connected to port 2. In this case, communication to port 2 can be disabled for all other ports.

Fabric Services

Because public devices are aware of the special fabric address, they can communicate with the fabric element and other devices connected to the fabric element. In fabric mode, each public device logs in to the following three services:

- the fabric (through fabric login, or FLOGI), to establish communication;
- the Simple Name Server (SNS), to add their information to the SNS directory;
- *and, if the device is an initiator,* the Registered State Change Notification service (RSCN), to receive notice when other devices change their power or communication status.

Note: Initiators include hosts (most common), bridges, routers, and intelligent storage systems.

Note: Devices on communication-disabled ports may appear in the SNS table even though zoning is supported.

After hosts log in to SNS, they request SNS directory information for all other connected devices. By maintaining names and addresses for each connected device through SNS, the Vixel 8100 helps hosts discover other devices. In multi-switch topologies, each Vixel 8100 maintains a complete SNS table by exchanging device information with other Vixel 8100s.

The Vixel 8100 establishes paths to other switches using RIP (Routing Information Protocol) 1.0, a routing algorithm commonly used in IP networking. Hops between switches are limited to 15.

Stealth Mode Operation

Addressing and Port Types

The Vixel 8100's patent-pending stealth mode uses only the Port portion of the Fibre Channel standard 24-bit address, setting the Domain and Area portions to zero. The Port portion represents each connected device as one or more Arbitrated Loop Physical Addresses (AL_PAs). Each Vixel 8100 switch is identified through a unique fabric number configured in SAN InSite.

The Vixel 8100 determines the appropriate route for device communications according to the 24-bit destination address (D_ID) embedded in the frame header sent by the device. The connected devices have no knowledge of other device locations or Vixel 8100 address routing mechanisms.

Note: I/O probes have traditionally been used by SCSI initiator hosts to discover SCSI targets. Hosts send Fibre Channel N_Port login (PLOGI) ELS frames to the 126-address loop address space.

I/O probes are supported in stealth mode. The Vixel 8100 sends the probe to the port configured to support the target (represented by an AL_PA). If this AL_PA has no connected devices, the Vixel 8100 routes the I/O probe to the fabric element, which responds to the I/O probe with a Link Services Reject (LS_RJT) frame, alerting the SCSI initiator that there are no devices at this address.

Stealth mode supports two port types: F_Port (for point-to-point connections) and StealthLoop.

AL_PA Address Set Allocation

For the switch to assign addresses, connected devices must support soft addressing. Connected devices are automatically assigned AL_PA address sets (each containing 1-10 AL_PAs) according to the following items:

- port configuration set through SAN InSite (type of port and connected device),
- the order in which the devices were discovered (in order from port 1 to port 8).

For example, the first host or RAID device discovered is assigned the 0x80 set of addresses while the second host or RAID discovered is assigned the 0x81 set of addresses.

Note: Address sets are divisions of the available private loop address space, which consists of 126 AL_PAs. The related Loop ID addresses are listed in "AL_PA — Loop ID Cross Reference Table" on page 29.

AL_PA Address Set(s) for Each Device Type and Port Type Configuration

Device Type	Port Type(s)	Order of Discovery								Max No. Devices	
		1st	2nd	3rd	4th	5th	6th	7th	8th	per switch	per port
Host	Stealth Loop, F_Port	0x80	0x81	0x82	0x84	0x88	0x04	0x08	0x0F	8	1
RAID**	Stealth Loop, F_Port	0x80	0x81	0x82	0x84	0x88	0x04	0x08	0x0F	8	1
JBOD8**	Stealth Loop	5X, 0xE0	DX, 0xE1	BX, 0xE2	3X, 0xE4	7X, 0xE8	none*	none*	none*	5	5
JBOD10**	Stealth Loop	4X	CX	6X	2X	AX	none*	none*	none*	5	5
Fabric	Stealth Loop, F_Port	9X	1X	7X	3X	BX	DX	5X	AX	8	1
Hub*** (XOR) #1	Stealth Loop	2X	Loss	3X	AX	BX	6X	7X	EX	1	1
Hub*** (XOR) #2	Stealth Loop	4X	Loss	5X	CX	DX				1	1

* Only five JBOD8 and five JBOD10 port types can be assigned per Vixel 8100 (no AL_PA sets are available for allocation to the sixth, seventh, or eighth connected JBOD devices).

**In SAN InSite, you can configure newly added storage devices (RAIDS or JBODs) to send LIPs to an initiator by enabling the "LIP If Storage Added" option under the desired initiator (including hosts and fabrics).

***Two Hub port types (#1 and #2) are allowed per switch. The JBOD port type can be used for hubs when the devices connected to the hub do not communicate with each other.

Note: The Vixel 8100 discovers devices when the configuration is loaded. Discovery occurs in sequence from ports 1-8.

AL_PA — Loop ID Cross Reference Table

Arbitrated Loop Physical Addresses								
AL_PA	Loop ID		AL_PA	Loop ID		AL_PA	Loop ID	
(hex)	(hex)	(decimal)	(hex)	(hex)	(decimal)	(hex)	(hex)	(decimal)
EF	00	0	A3	2B	43	4D	56	86
E8	01	1	9F	2C	44	4C	57	87
E4	02	2	9E	2D	45	4B	58	88
E2	03	3	9D	2E	46	4A	59	89
E1	04	4	9B	2F	47	49	5A	90
E0	05	5	98	30	48	47	5B	91
DC	06	6	97	31	49	46	5C	92
DA	07	7	90	32	50	45	5D	93
D9	08	8	8F	33	51	43	5E	94
D6	09	9	88	34	52	3C	5F	95
D5	0A	10	84	35	53	3A	60	96
D4	0B	11	82	36	54	39	61	97
D3	0C	12	81	37	55	36	62	98
D2	0D	13	80	38	56	35	63	99
D1	0E	14	7C	39	57	34	64	100
CE	0F	15	7A	3A	58	33	65	101
CD	10	16	79	3B	59	32	66	102
CC	11	17	76	3C	60	31	67	103
CB	12	18	75	3D	61	2E	68	104
CA	13	19	74	3E	62	2D	69	105
C9	14	20	73	3F	63	2C	6A	106
C7	15	21	72	40	64	2B	6B	107
C6	16	22	71	41	65	2A	6C	108
C5	17	23	6E	42	66	29	6D	109
C3	18	24	6D	43	67	27	6E	110
BC	19	25	6C	44	68	26	6F	111
BA	1A	26	6B	45	69	25	70	112
B9	1B	27	6A	46	70	23	71	113
B6	1C	28	69	47	71	1F	72	114
B5	1D	29	67	48	72	1E	73	115
B4	1E	30	66	49	73	1D	74	116
B3	1F	31	65	4A	74	1B	75	117
B2	20	32	63	4B	75	18	76	118
B1	21	33	5C	4C	76	17	77	119
AE	22	34	5A	4D	77	10	78	120
AD	23	35	59	4E	78	0F	79	121
AC	24	36	56	4F	79	08	7A	122
AB	25	37	55	50	80	04	7B	123
AA	26	38	54	51	81	02	7C	124
A9	27	39	53	52	82	01	7D	125
A7	28	40	52	53	83	00	7E	126
A6	29	41	51	54	84	---	7F	127
A5	2A	42	4E	55	85			

Note: To attach a loop of hosts, configure the port as Fabric device type and Stealth Loop port type.

Because fabrics and hubs draw from the same address sets as do JBOD8s and JBOD10s, you may need to choose between these device types. For example, if two fabric devices are already allocated and you want to allocate another fabric, the third fabric discovered is given the 7X address set. Because the 7X address set is no longer available for the fifth JBOD8 device, only four JBOD8 devices are now allowed on this switch. In this example, you would need to choose between the following configurations:

- Three fabric devices and four JBOD8 devices.

  OR
- Two fabric devices and five JBOD8 devices.

Note: JBODs are target devices; they do not initiate communication to other devices. JBOD ports are designed to funnel all frames into the switch for distribution to initiator devices. This design allows stealth to allocate several AL_PA addresses to one port.

To connect a device whose attached nodes communicate with each other on their own segment, configure the port as one of the following device types:

- Fabric (with Stealth Loop port type) or
- Hub.

To connect a hub (such as Vixel's R1000 or R2000), configure the port as one of the following device types:

- Fabric (with Stealth Loop port type) or
- Hub or
- One of the JBOD device types (JBOD8 or JBOD10), if the hub's attached nodes do not communicate with each other on their own segment.

The Hub device type consumes several addresses because it is designed for hub XOR devices, which have a bit-oriented masking nature. When a hub XOR device consumes an address set, all other address sets that use the same bit become unavailable. (All address sets in the Hub XOR #1 and Hub XOR #2 rows use the same bit). When another device type, such as a JBOD10, consumes an address set, it uses the address set's value rather than its bit. Therefore, other address sets with this bit are available. (Notice that the first discovered JBOD10 uses the 4X address set, which could be used by Hub XOR #1; however, other address sets with this bit are available).

A hub can have up to ten attached devices, including both targets and initiators.

Zoning

Both fabric and stealth modes support port zoning, which allows groups that share a fabric topology to keep their data separate. For example, human resources may not want other departments to be able to access sensitive data on devices connected to port 2. In this case, communication to port 2 can be disabled for all other ports.

Back-up Ports

In stealth mode, you can set a back-up port to ensure a failover path for connected devices. Remember to reset the switch when you want to reestablish connection to the primary port.

Benefits to Private Loops

Stealth mode benefits private (arbitrated) loops:

- Increased bandwidth: instead of all sharing 100 Mbyte bandwidth, the devices can be segmented into loops (by port) that each have their own 200 Mbytes.
- Enhanced throughput: pairs of ports can communicate simultaneously, mitigating the blocking nature of the arbitrated loop.
- Decreased system disruption: the LIPs (loop initialization primitives) that result from adding and removing devices affect a single fabric port only. (LIPs are also sent to hosts for which you have enabled the “LIP If Storage Added" option.)

Segmenting Private Loops

Stealth mode allows you to segment a private loop of up to 119 devices that do not yet support public loops into multiple loops—each with its own 200 Mbytes bandwidth—then interconnect the multiple loops. As shown in Figure 4-1 below, these multiple-loop topologies allow you to isolate one or more devices on a Vixel 8100 port.

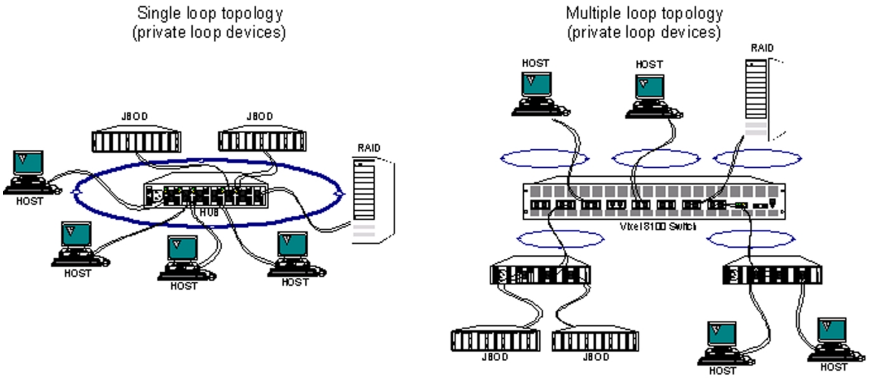


Figure 4-1 *With the Vixel 8100 stealth mode, devices can migrate form a single loop topology to a multiple loop topology.*

Mixing Fabric-Attached and Loop Devices

Note: In stealth mode, Vixel 8100 ports can be configured as either StealthLoop or F_Port. Fabric-attached (N_Port) devices connect to F_Port-configured ports.

As shown in Figure 4-2 below, Vixel 8100 stealth mode allows you to mix private loop devices with N_Port—or "fabric-attached"—single AL_PA devices (such as RAIDs) that perform fabric login. This flexible topology improves the performance of host-to-storage interconnection by providing dedicated bandwidth and eliminating loop arbitration delay.

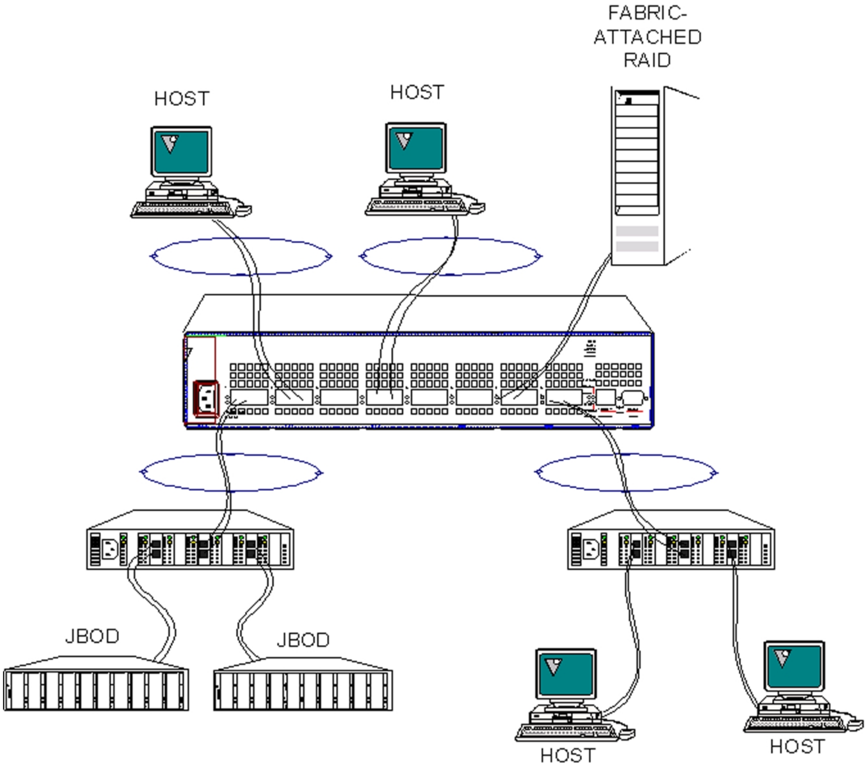


Figure 4-2

Configuring Multi-Switch Topologies

Multi-switch topologies consist of a *root* switch (central control that routes all switch traffic) and cascaded *remote* switches.

Only the root switches can support JBODS and hubs (devices that use multiple AL_PAs). Remote switches are restricted to hosts or RAIDs (devices that use only one AL_PA). Hosts can access any storage on the fabric (such as RAIDs, JBODs, and hubs).

Hosts can access RAIDs, JBODs, and hubs through the root switch and other remote switches. They can also access their own local RAIDs.

As shown in the next table, each possible multi-switch topology supports a different number of devices. The eight addresses consumed by each additional remote switch was taken from the JBOD8 column; however, the JBOD10 column can also be used, with the understanding that two of the ten allocated addresses are unused. Each JBOD8, JBOD10, or Hub/XOR port consumes addresses that could be used by hosts or RAIDs.

Remote Fabrics (Topology No.*)	**Interconnected Hubs/ XORs**	Maximum number of supported Hosts/RAIDS	Maximum number of supported JBOD10s	Maximum number of supported JBOD8s
0	0	8	5	5
1	0	14	5	5
2 (2a)	0	20	5	5
2 (2b)	1	13	2	2
2 (2c)	2	12	0	0
3	0	26	5	4
4	0	32	5	3
5	0	38	5	2
6	0	44	5	1
7	0	50	5	0
8	0	56	0	0

*Topology numbers are displayed in Figure 4-3 below.

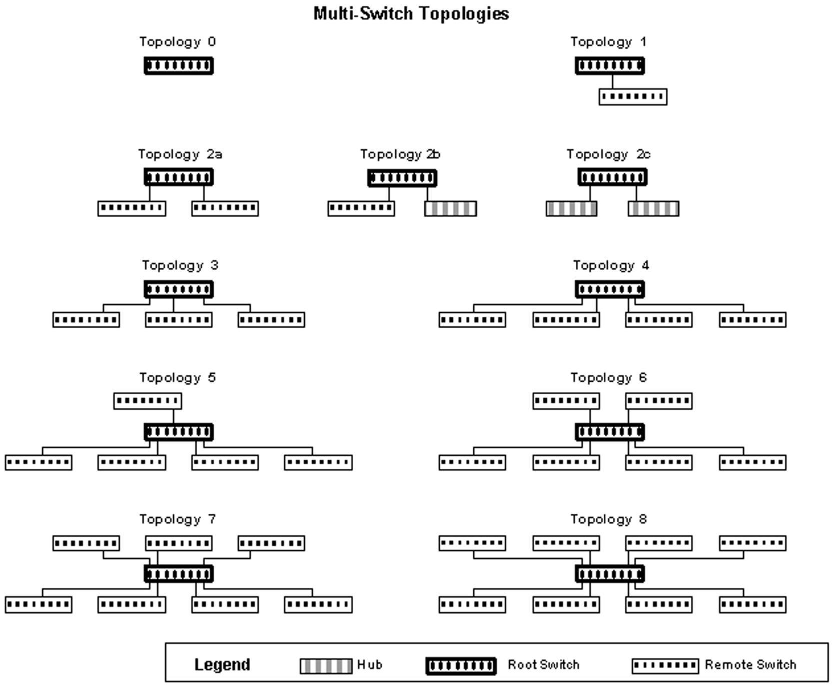


Figure 4-3

Figure 4-4 below displays an example of devices that can be connected in a topology 3 configuration. In this example, the root fabric has a total of 21 AL_PA's: 3 hosts + a 10-drive JBOD + an 8-drive JBOD. The remote fabrics use 7 AL_PA's each, which are taken from the AL_PA sets for FABRIC object types. The entire configuration uses 35 AL_PA's.

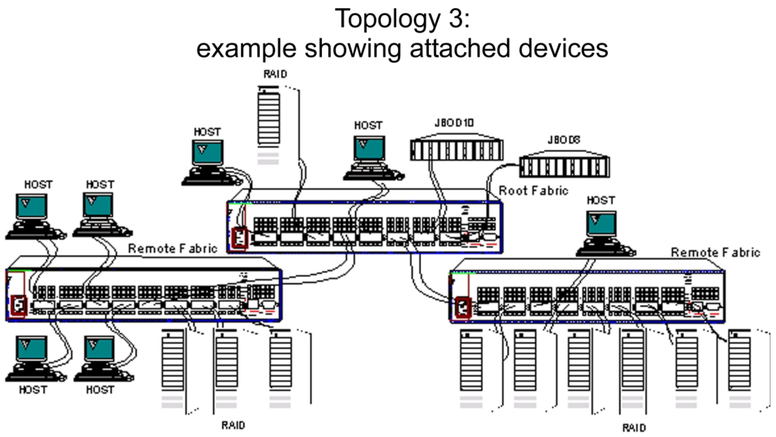


Figure 4-4

Figure 4-5 below displays an example of devices that can be connected in a topology 10 configuration. In this example, a root fabric supports one remote fabric and two hubs ("Hub #1" and "Hub (Cascaded)"). Notice that the JBOD10 devices attached to "Hub #1" do not communicate with each other while the host and JBOD8 devices attached to "Hub (Cascaded)" do communicate with each other (implied by the double arrows); to conserve AL_PAs, the port to which "Hub #1" is connected (port 7) is defined as a JBOD10 port type with a quantity of two. Port 6, the port for "Hub (Cascaded)," is defined as a Hub port type.

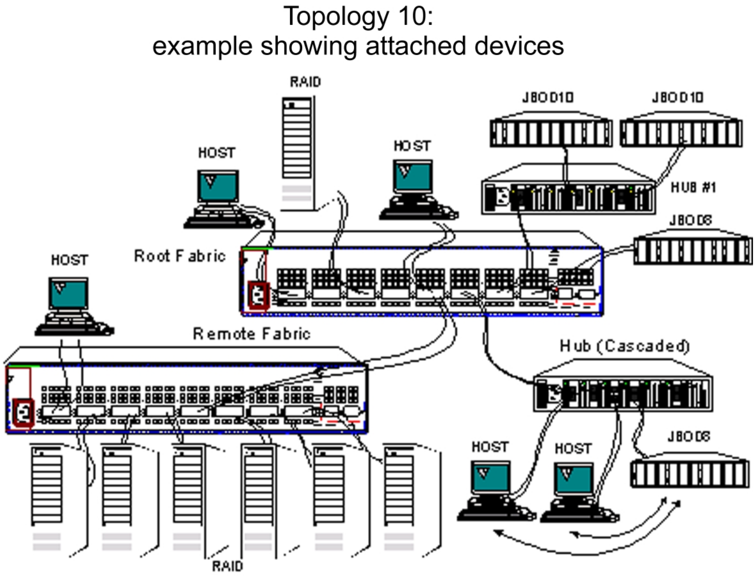


Figure 4-5

CHAPTER 5 Troubleshooting

Understanding Start-up (POST) LED Sequence 36

Running POST Diagnostics 38

Answers to Common Questions 40

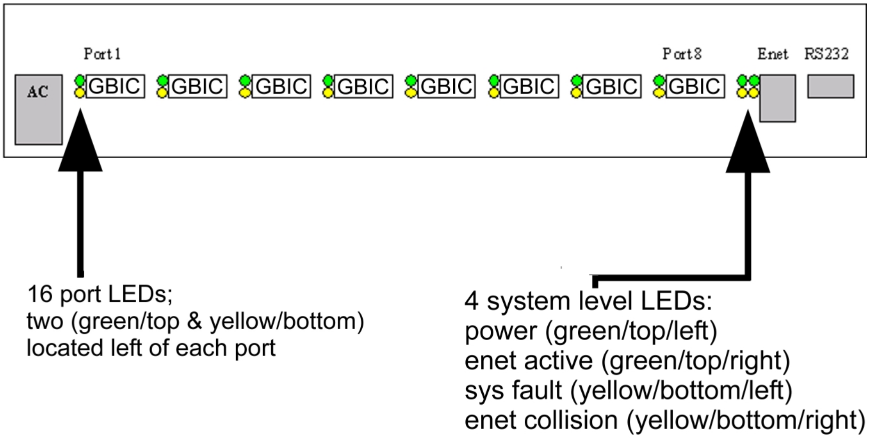
You can check the system and port status through the Vixel 8100 LEDs.

During Power On Self Test (POST), the system LEDs indicate whether POST has passed or failed, and each port LED indicates whether a particular subtest has passed or failed. During run-time, all LEDs indicate general health status.

The management (MGMT-RS-232) port supports Vixel 8100 post diagnostics when connected to a standard terminal with a terminal emulator.

Understanding Start-up (POST) LED Sequence

The Vixel 8100 has 16 port LEDs (two for each port) and 4 system LEDs, as shown below.



Port1
Port8
Enet
RS232
AC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
GBIC
16 port LEDs;
two (green/top & yellow/bottom)
located left of each port
4 system level LEDs:
power (green/top/left)
enet active (green/top/right)
sys fault (yellow/bottom/left)
enet collision (yellow/bottom/right)

Figure 5-1

When the Vixel 8100 is started up, the power and fault LEDs are the only LEDs in a known state—all other LEDs are unknown and must be initialized. The power-fault combinations and their indications are listed below.

Power LED	Fault LED	Indication during POST
Off	Off	FPGAs failed to load or the power to Vixel 8100 is inadequate.
Solid	Off	Normal operation.
Off	Solid	CPU did not get started; bus integrity problem. Contact an authorized service person.
Solid	Solid	CPU starts but system abilities are limited.

The Vixel 8100 runs through Power On Self Test (POST) diagnostics to verify the fundamental integrity of the Vixel 8100 box, port memory (flash and SDRAM), and related circuitry. The POST sequence follows.

1. All LEDs turn solid for one second.
2. In sequence from left to right, each green port LED turns solid during a major POST test. (Length of time varies for each test.)
3. *If (a) all green port LEDs have turned solid then off and (b) all LEDs then turn off,* the Vixel 8100 has passed all POST tests and is ready for operation.
   If one or more yellow port LED blinks, the Vixel 8100 has failed the POST test(s) corresponding to the blinking LED below.

Note: For a list of LED indications during operation, see “Ports and LEDs” on page 3.

Port Number	POST Test Failed
1	RAM
2	RTC
3	LOAD_INIT
4	DUART
5	LOAD
6	EPROM
7	FPP
8	FCPORT

Run POST diagnostics to find the numbers of the failed subtest and error code.

Running POST Diagnostics

CAUTION: Run this mode only under the direction of an authorized service person.

To display test results, you can put the Vixel 8100 into a diagnostic output mode. In this mode, the diagnostic displays a passed or failed result and prompts you with additional options.

To put the Vixel 8100 into optional diagnostic output mode:

1. Obtain:
    - a serial DB-9 null-modem cable
    - an asynchronous terminal (19,200 baud, 8 bit, 1 stop, no parity), or a PC in terminal emulation mode.
2. Power off the Vixel 8100.
3. Insert serial cable into the Vixel 8100 MGMT port (on the GBIC side), connecting one DB9 end to an asynchronous terminal or to a PC in terminal emulation mode (using Microsoft Windows' HyperTerminal).

    If you plan to run the Diagnostic External LoopBack Test, be sure that you have the necessary copper or optical Fibre Channel loopback plugs and be sure that you insert them before powering the Vixel 8100 on.
4. Power on the Vixel 8100.

5. While the Port 1 green LED is on, press **Enter** repeatedly.

   You will see an information display similar to the following. Be prepared to discuss the results with an authorized service person.

```
---------------------------------------------------------
     VIXEL Model R8100           VIXEL Corporation(TM)
     POST Revisions: 01.00 00
               Diagnostic Analysis
---- Devices ---------------------- Result - Information -
 Flash Memory Checksum ............ PASSED
 SDRAM Memory (16M)................ PASSED
 Real Time Clock (RTC) ............ PASSED
 Dual Asynchronous (DUART) ........ PASSED
 Ethernet Device .................. PASSED
 Route Timer/Table/Address Devices. PASSED
 Port Control Devices ............. PASSED
 FPP Devices ...................... PASSED
 Internal Port Loopback Tests ..... PASSED
 Parity Analysis .................. PASSED
 Fan 1,2 & 3 Status................ PASSED

<< Diagnostic Options Menu >>
 Option 2 System must be Rebooted.
 1) FPP Diagnostic Testbench
 2) Switch Boot to Alternate Image
 3) Set MGMT Port to NVRAM Utility
 4) Continue System Boot to Switch
   Select System Diagnostic Option :
```

Description of Diagnostic Options

Note: Option #4 is automatically activated if no option is selected within 30 seconds.

1. FPP Diagnostic Testbench

   This option allows you to select and execute diagnostic tests such as the external loopback test, which verifies that the port GBICs are operational. This option also tests the external port hardware. Either copper or optical Fibre Channel loopback plugs are needed to conduct this test.

2. Switch Boot to Alternate Image

   This option lets you switch firmware. (An alternative method is to do this through San InSite; see San InSite online help.) The Vixel 8100 allows for two boot images of the firmware to be stored in flash memory. "Image 1" is the latest version at the time of manufacture and is installed in the factory. "Image 2" comes from the factory initially empty. This is in preparation for letting you download a newer copy of the firmware at a later time, if necessary, into the proper flash location.

3. Set MGMT Port to NVRAM Utility

   At the direction of an authorized service person, this test option offers you a means to change the Vixel 8100's IP address. It disables the MGMT port's normal function and enables a NVRAM utility program.

   You must re-enable the normal MGMT port operation through the NVRAM utility when you are through running NVRAM mode. You must also select diagnostic option 4 (Continue System Boot to Switch).
4. Continue System Boot to Switch

   Returns the Vixel 8100 to normal operation.

Diagnostic "FAILED" Test Codes

In Diagnostic Print Mode, "FAILED" messages include four bytes, each indicating—in sequence—the major test category, failed port number, subtest number, and overall error code.

For example, in the message:

```
Port #4 . . . . . . . . FAILED 05 04 03 10
```

the bytes 05, 04, 03, and 10 indicate failure of the following items:

- major test number 5 (FPP)
- port number 4
- subtest number 3 ((FPP FIFO BIST)
- overall error code 10 (FF BAD BIST RX)

For further information, contact an authorized service person.

Answers to Common Questions

If you have a problem, make sure you read the fault messages in the message log. Common questions and answers follow.

The attached host cannot communicate with a remote device.

This inability to communicate could mean one of three things:

1. The remote device is not connected.

   Check that the port LEDs are working for both the host and the remote device.
2. The remote device link is not active and the port LED is blinking.

   A blinking port LED means that the communications link either has not been established or has ceased communication; there could be a possible configuration problem. Check that you've correctly specified the port type to match the device type; see the Configuration Stealth tab port definitions in the San InSite User's Guide, or see the online help documentation available in SAN InSite.

3. Frames are being rejected from the local device to the remote device (this would be detected and reported via SNMP, in the Link Status view). In this case, check one of the following:
   - Make sure ports are configured correctly for the proper devices and that the Stealth Route Table was set up properly.
   - If configured in the stealth mode and a host cannot recognize the storage, reboot the host.

I have connected an optical device to the correct port on the Vixel 8100 but the port LED isn't on. I know that the device works and I know that the cable type matches the port/GBIC type.

Make sure that you have correctly polarized (crossed) the receive and transmit ends of an optical cable into their respective receive and transmit receptacles, both on the device end and the Vixel 8100 end. (Optical cables are not automatically polarized as copper cables are.)

Note: On an optical port, receive is on the left while transmit is on the right.

If the receive and transmit receptacles are not marked or indicated by bracket enclosures, cross the printed side of the wiring with the unprinted side. For example, at the receive socket in the device end, plug in the *printed* side of the wiring; at the receive socket in the Vixel 8100 end, plug in the *unprinted* side of the wiring.

I'm trying to connect an optical cable to a port, but something's wrong with the port: the cable won't fit into the receive/transmit receptacles on the port.

Be sure that you remove all port dust covers/plugs that were shipped with the optical ports on the Vixel 8100. Some types of dust plugs that fit into the receive/transmit receptacles of some types of optical ports do in fact resemble a connector. Just pull them out gently with fingertip pressure, then cable the device to the port.

I'm seeing some strange results with a port; sometimes the device and Vixel 8100 communicate and sometimes not.

If you have a copper port, be sure that you have firmly attached the copper cable to the Vixel 8100 port and that you've properly tightened both screws on both ends of the cable connector. Otherwise, a loose connection can cause sporadic results.

If you have an optical port, swap out the cable. Optical cables, if bent more than the recommended radius (maximum radius is no more than three inches), can break, causing sporadic results. Bending can also add attenuation, which could result in signal loss.

WARNING: GBICs emit invisible laser radiation. Do not stare into the transmitted beam.

CHAPTER 6

Technical Reference

Default Switch Settings 42
Technical Support 45
Fibre Channel References 45

Default Switch Settings

The Vixel 8100 is shipped with the default settings shown below (as displayed in the MIB, or Management Information Base; an SNMP device management structure).

You do not need to change the configuration if it is suitable for your topology. If you do need to customize the configuration, use configuration options in SAN InSite to define the device connections to the Vixel 8100. See the SAN InSite documentation for instructions.

SNMP Community Names for read only and read-write

Note: SNMP community names are available through the MIB only.

SNMP Community Ro	"public"
SNMP Community Rw	"private"

IP Address, Net Mask & Gateway for this switch

Slip IP Addr	192.168.2.129
Slip IP Net Mask	255.255.255.0
Enet IP Net Addr	192.168.1.129
Enet IP Net Mask	255.255.255.0
Enet Default Gateway	0.0.0.0
Sys Domain	0x00
Sys Fabric Name	"8100 Fabric"
Sys Hold Time	5 seconds
SysBootImage	Image 1

Port Configuration

Fport Name	"Port 1" through "Port 8"
Fport Rx Buf Size	2112 Bytes
Fport EDTOV	0.5 seconds
Fport RATOV	120 seconds
Fport ALTIME	15 milliseconds
Fport Cos Supported	Class 2 and 3 support.
Fport Type	Ports 1-8 Stealth Loop

Port Zoning Configuration Table

Zoning allows groups that share a fabric topology to keep their data separate. (For example, human resources may not want other departments to be able to access sensitive data.) Fabric ports can be authorized or prevented from accessing devices on other ports. The following default configuration allows ports 1-4 to talk to all other ports. Ports 5-8 can only talk to ports 1-4. (A cell containing "X" indicates that the ports corresponding to the cell's row and column can communicate.)

Port	1	2	3	4	5	6	7	8
1		X	X	X	X	X	X	X
2	X		X	X	X	X	X	X
3	X	X		X	X	X	X	X
4	X	X	X		X	X	X	X
5	X	X	X	X				
6	X	X	X	X				
7	X	X	X	X				
8	X	X	X	X				

Route Configuration

Default Route Port Prim	0
Default Route Port Backup	0
Stealth Local Fabric Number	0

Stealth Route Entry

Under the default route configuration, you can attach up to 20 JBOD drives (total) to ports 1-4 and up to 7 hosts to ports 5-8.

Ports	Type	JBOD10	JBOD8	Hubs	Fabric	Backup	LIP
1	JBOD	2	0	1	0	0	False
2	JBOD	1	1	1	0	0	False
3	JBOD	1	1	1	0	0	False
4	JBOD	1	1	1	0	0	False
5	Fabric	0	0	1	1	0	True
6	Fabric	0	0	1	2	0	True
7	Fabric	0	0	1	3	0	True
8	Fabric	0	0	1	4	0	True

The default route configuration allocates enough AL_PAs for ports 1-4 so that two ten-drive JBOD cabinets can be attached to each port. Enough AL_PAs are allocated for ports 5-8 so that 7 hosts can be attached per port. No backup ports are configured. Ports 5-8 will be LIPed when storage is added to ports 1-4. In this configuration the values in the "Hubs" column are ignored.

Image Download Configuration

Tftp Host IP	0.0.0.0
Tftp File	No default string.
Tftp Gateway Ip	None.

System Message Log

Note: In SAN InSite, the “System Message Log” settings are seen in the 8100 Configuration dialog box (Logging tab) and in the 8100 Event Log.

Log Severity Filter	Notify.
Log Fault LED Severity	Critical.

Technical Support

Before you contact Vixel Technical Support, make sure you check for solutions in this guide. Also check with your network administrator. Vixel Technical Support's contact information is below.

Vixel Corporation, 11911 Northcreek Parkway South, Bothell, WA 98011

Phone:(888)881-6085
Fax:(425)806-4502
E-mail:support@vixel.com

Fibre Channel References

The following books give useful information about Fibre Channel.

- Alan F. Benner, *Fibre Channel*. McGraw-Hill, 1996. ISBN 0-07-005669-2.
- Tom Clark, *Designing Storage Area Networks*. Addison Wesley Longman, Q3 1999.
- Jan Dedek, *Fibre Channel - The Basics*. ANCOT Corporation, 1997. ISBN 0-9637439-3-7.
- Robert Kembel, *Arbitrated Loop*. Connectivity Solutions, 1996. ISBN 0-931836-82-4.
- Robert Kembel, *A Comprehensive Introduction*. Connectivity Solutions, 1998. ISBN 0-931836-84-0.

APPENDIX A Event Messages

An event message may indicate that there is a problem with an attached device, or that a configuration value specified for a device is invalid, or that there may be a problem internal to the Vixel 8100, or it may simply note that a device that was offline is again online.

The following Event Message tables list possible event messages (hardware status messages first, then system status messages) and explain the likely cause as well as the action required, if any, if such a message does occur. These messages fall into one of the following categories, which indicate the level of urgency for each message, from most to least severe:

1	Emergency	immediate intervention needed; system failing
2	Alert	unrecoverable condition reported; major event in progress
3	Critical	event failed with possible loss of integrity
4	Error	condition failed; needs intervention to correct
5	Warning	failed event occurred; no recovery needed
6	Notify	event rejected and/or ignored
7	Info	event occurred; no action needed
8	Debug	internal message for development
9	Mark	message marker

Some of the messages have various symbols embedded. The symbols and their meanings are as follows:

<table>
<tr><td>{ }</td><td>Strings or values that are substituted at the specified location in the message</td></tr>
<tr><td>“ “</td><td>A possible ‘No string’ at the specified location in the message</td></tr>
<tr><td>|</td><td>One of the specified settings is displayed</td></tr>
<tr><td>-</td><td>One value within the range of numbers is displayed</td></tr>
<tr><td>[ ]</td><td>Type of string or value substituted at the specified location in the message</td></tr>
</table>

Emergency Messages

Event Message	Meaning	Action
Fan {1-3} has stopped, AirFlow Status {Insufficient | Nominal | Maximum | Critical}	The status of a system fan has changed.	If airflow status is insufficient or critical, unit must be serviced by an authorized service representative.
MEMORY ERROR [hex value]	POST detected a hard failure in memory.	Unit must be serviced by an authorized service representative.
Real Time Clock NMI Test Failure	POST has detected a nonmaskable interrupt error.	Cycle the power off and on*
SYSCONF ERROR [hex value]	An error occurred while the switch was loading the system configuration during powerup.	Unit must be serviced by an authorized service representative.
SCHEDULER FAILED	A low-level software error has occurred.	Unit must be serviced by an authorized service representative.
SCHEDULER STALLED	A low-level software error has occurred.	Unit must be serviced by an authorized service representative.
Fabric Element Received invalid frame format	An event has occurred on the switch control port that has caused that port to become disabled.	Power cycle the switch and call an authorized service representative.

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

Alert Messages

Event Message	Meaning	Action
Fabric Element Receive Dma Parity Error	A fabric element DMA receive error occurred.	Monitor carefully*
Fabric Element Transmit Dma Parity Error	A fabric element DMA transmit error occurred.	Monitor carefully*
FPGA Load failed	POST detected an error during an FPGA Load operation.	Reboot*
I960 Bus Parity Error	A bus parity error occurred.	Monitor carefully*
{MGMT | UPS} Port failed, test {1-15}	POST detected a failed serial port.	Check the Vixel 8100 Panel window for the specific failed port; unit must be serviced by an authorized service representative.
Parity Error during Diagnostics detected	POST detected a parity error during diagnostics.	Reboot*
Port {1-8} Encoder/ Decoder failed	POST detected an error on the (Encoder/ Decoder).	Reboot*
Port {1-8} Loopback failed	POST detected an error in the Loopback diagnostic.	Reboot*
Port {1-8} Port Control Parity Error	A port control bus parity error occurred.	Monitor carefully*
Port {1-8} Port Control failed	POST detected a port control error.	Reboot*
Port {1-8} Port Control Tag Error	A port control tag error occurred.	Monitor carefully*
Real Time Clock Battery Low	POST has detected that the real-time clock's battery is low.	Unit must be serviced by an authorized service representative.
Real Time Clock New NvRam	POST has detected a NVRAM error.	Cycle the power off and on*

Alert Messages (Continued)

Event Message	Meaning	Action
Real Time Clock NvRam Test Failure	POST has detected a nonvolatile RAM error.	Cycle the power off and on*
Ethernet Port failed, test [n]	POST has detected a failure in the ethernet test.	Unit must be serviced by an authorized service representative.
Ethernet Receive Parity Error	A parity error has been detected in the ethernet interface.	Monitor carefully*
Ethernet Transmit Parity Error	A parity error has been detected in the ethernet interface.	Monitor carefully*

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

Critical Messages

Event Message	Meaning	Action
Temperatures over limit	System temperature has exceeded operational thresholds.	Unit must be serviced by an authorized service representative.
RTC Battery exhausted	The system’s real-time clock battery is no longer functional.	Unit must be serviced by an authorized service representative.

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representativerepresentative.

Error Messages

Event Message	Meaning	Action
{Cfg | Html | Fpga | Code} flash update {" " | start} failed, [hex value]	An attempt was made to save a firmware update to flash (nonvolatile) memory and failed, either at the start of or during the update.	Save it again*
Loop Arbitration generated no Address, Port {1-8}	Another device has control of the loop. Can prevent this switch from operating in stealth mode.	Possible reconfiguration.
System configuration save {" " | start} failed, [hex value]	An error occurred either while the switch was saving the configuration to flash memory or while trying to start the system configuration.	Retry*
Tftp Bad Download Version, [hex value]	The switch detected that the firmware being downloaded was corrupted from a possible transmission error.	Retry*
Tftp Download Too Large, Blk [value] Len [value]	A size (length) error occurred while firmware was being downloaded.	Retry*
Tftp Download Error, {Bad Type | No Resources | Timeout | Use Message | No File | Access | Disk Full | Illegal Op | Bad TID | Exists | No User}	A TFTP error occurred.	Check the message indicated. Also, check for a TFTP error and check the TFTP configuration of the Vixel 8100 and/or the TFTP server.

Error Messages (Continued)

Event Message	Meaning	Action
SRoute {1-8}, unexpected stealth route type [hex value]	A port's stealth route type is being set to an invalid value.	Retry*

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

Warning Messages

Event Message	Meaning	Action
L_Port {1-8}, [portname], linkdown	In a loop topology, the switch sends this message indicating that a link is down and waiting for reinitialization. Can indicate that a new device was inserted in the loop or that a device has detected an error only recoverable by reinitialization, or that a host device can't complete a disk access so it brings the unit "down" to wait for reinitialization.	None

Warning Messages (Continued)

Event Message	Meaning	Action
F_Port {1-8}, [portname], linkdown	In a point-to-point topology, the switch sends this message indicating that a link is down and waiting for reinitialization. Can indicate that a new device is connecting, or that a device has detected an error only recoverable by reinitialization, or that a host device can't complete a disk access so it brings the unit "down" to wait for reinitialization.	None
Port {1-8}, [portname], link failure	The switch reports an external failure on one of the links. Typically, this is a loose or disconnected cable from the Fibre Channel port.	If this message is followed by a port "linkup" message, the Vixel 8100 has recovered and no action is required. If not, check device cabling on the loop.

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

Notify Messages

Event Message	Meaning	Action
Port {1-8} type must be {Fport | FLport or StealthLoop | Fport, FLport, or StealthLoop}	Displayed when the Stealth Configuration menu has been loaded. It indicates that a port has been set to an invalid value.	Correct the value in the SAN InSite Vixel 8100 Configuration dialog box.
Port {1-8} type not allowed for {non- | " "} stealth route {mode | none | fabric | host | raid | jbod | hub | type}	Displayed when the Stealth Configuration menu has been loaded. It indicates that the specified port value is invalid for this configuration.	Correct the value in the SAN InSite Vixel 8100 Configuration dialog box.
Sroute {1-8} cannot backup sroute {1-8}, too many	In stealth mode, the specified backup port cannot backup the primary port because it is already backing up another port.	Change the port's primary backup port.
Sroute {1-8} has duplicate type, "fabric {1-8} {(Main) | " "}"	In stealth mode, the specified port has a duplicate type.	Change the fabric type to another type.
Sroute {1-8}, stealth {hub | jbod} type invalid on this switch	In stealth mode, the specified type is invalid for this particular switch because the switch is not the main fabric.	Change the device type to another type.
SRoute {1-8}, Backup port's type {must be None | must match the primary}	In stealth mode, the backup port's type must be as noted.	Change the port type to another type, as indicated.
SRoute {1-8}, "fabric {1-8}" type invalid on this switch	In stealth mode, the specified fabric type is invalid on this particular switch.	Change the fabric type to a valid type.

Notify Messages (Continued)

Event Message	Meaning	Action
SRoute {1-8}, Root fabric type invalid on this switch	In stealth mode, the user is trying to designate this switch as the root switch, but there are other connected switches that are already designated as "Root."	Change connected switches to be non-root first, then change this switch to "Root."
SRoute {Primary | Backup} default route not set to fabric port {1-8}	In stealth mode, the specified default route is not set to the correct port.	Change the specified default route as indicated.
SRoute, switch needs Root fabric port	A root switch has not been designated.	Designate a root switch.
SRoute, Too many {hub | fabric | jbod}{s | 10s | 8s}, cannot exceed [value]	In stealth mode, the specified number of fabrics/devices has exceeded the allowable value.	Change the configuration accordingly.
User restarted Port {1-8}, [portname]	Indicates that a port was restarted through SNMP .	None
User shutdown Port {1-8}, [portname]	Indicates that a port was shut down through SNMP.	None
Temperature OK	System temperature has returned to normal.	None
RTC Battery OK	Real-time clock battery voltage level is normal.	None
PubMode: Port {1-8} type must not be stealth-Loop	User is attempting to change from stealth mode to fabric mode, but the named port has an invalid configuration.	Change the specified port's type to a valid port type for fabric mode.

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

Info Messages

Event Message	Meaning	Action
Fan {1-3} has returned, AirFlow Status {Insufficient | Nominal | Maximum | Critical}	A fan has returned to operation.	If airflow status is insufficient or critical, unit must be serviced by an authorized service representative. If airflow status is nominal or maximum, no action is needed.
L_Port {1-8}, [portname], linkup	Confirms that the link is again up.	None
Message log cleared	Confirms that the user cleared the message log.	None
F_Port {1-8}, [portname], linkup	An F_Port has initialized and is up.	None

* Under normal operation this error should never occur. In the unlikely event that it does, or persists, contact an authorized service representative.

APPENDIX B Glossary

AL_PA or Arbitrated Loop Physical Address	A one-byte value used to identify a port in an Arbitrated Loop topology. The value of the AL_PA corresponds to bits 7:0 of the 24-bit Native Address Identifier.
Arbitrated Loop	A Fibre Channel topology structured as a loop and requiring a port to successfully arbitrate prior to establishing a circuit to send and/or receive frames.
Arbitration	The process of selecting one respondent from a group requesting service at the same time.
Close (CLS)	An Arbitrated Loop protocol used to terminate a loop circuit.
Copper Cable	Cables used to connect storage modules and host-bus adapters with copper interfaces to copper GBICS. Best suited for intra-cabinet. Best cable types include twin-axial and equalized. Intra-cabinet copper cables should not exceed 13 meters.
Current Fill Word	The fill word that the Loop Port State Machine uses when a fill word is to be transmitted.
Duplex Cable	Two fiber cables suitable for duplex transmission.
Full-Duplex Transmission	Transmission in both directions, simultaneously (transmitting on one, receiving on the other).
Fiber Optics	Light transmission through optical fibers for communication or signaling
Fibre Channel	Fibre Channel is a 1 gigabit per second data transfer interface technology that maps several common transport protocols including IP and SCSI, allowing it to merge high-speed I/O and networking functionality in a single connectivity technology. Fibre channel is an open standard as defined by ANSI and OSI standards and operates over copper and fiber optic cabling at distances of up to 10 Kilometers. It is unique in its support of multiple inter-operable topologies including point-to-point, arbitrated-loop and switching and it offers several qualities of service for network optimization. With its large packet sizes, Fibre Channel is ideal for storage, video, graphic and mass data transfer applications.

GBIC	Giga-Bit Interface Converter Module. Open Standard developed by Vixel Corp., Sun, Compaq, and Amp. Industry's first hot pluggable, gigabit transceiver.
HSSDC connector	High Speed Serial Data Connector. Used on GBICs and Host Bus Adapters.
Mb/s	Megabits per second, 1,024,000 bits per second.
MB/s	Megabytes per second, 8,192,000 bits per second. One byte = 8 bits
Multimode Fiber	An optical waveguide in which typical core/cladding sizes are 50/125 and 62.5/125 microns.
Longwave	Refers to wavelength or frequency in the spectrum of light. Specified under Fibre Channel as 1310 nm is the operating range of long wavelength lasers. The maximum distance for longwave is 10 kilometers.
Loop Port State Machine (LPSM)	A logical entity which performs the Arbitrated Loop specific protocols.
Node	An entity with one or more N_Ports or NL_Ports.
OFC	Optical Fiber Control. A safety interlock system that controls the optical power level in an open fiber optic cable. Not supported in GBICs.
Open	An Arbitrated Loop protocol used to establish a loop circuit.
Protocol	A data transmission convention which may include timing, control, formatting, error detection with correction and data representation.
SC Duplex Connector	Standard Fibre Channel terminating connector for fiber (short-wave and long-wave). Used to plug into GBIC and Host Bus Adapter.
SCSI	Small Computer System Interface. Standard interface for storage modules.
Shortwave	Refers to wavelength or frequency in the spectrum of light. Specified under Fibre Channel as 780- 860 nm it is the operating range of short wavelength lasers. The maximum distance for shortwave is 500 meters.
Single Mode Fiber	An optional wave guide in which typical core/cladding sizes are 9/125 microns.

Topology	The logical and/or physical arrangement of stations on a network. Fibre Channel topologies include point-to-point, Arbitrated Loop, and switched fabric.

Index

D

Default Switch Settings 42
Diagnostic “FAILED” Test Codes 40
Diagnostic Options 39

E

Environmental Requirements 2
Ethernet Port 2
Event Messages 46

F

Features 1

G

GigaBit Interface Converters (GBICs) 3
    Inserting and Removing 13
Glossary 57

I

Installing 8
Introduction 1

L

LEDs 3
    During Operation 3
    During Start-up (POST) 12

O

Operation
    Theory of 25

P

Ports 3
POST Diagnostics, Running 38
Power Supply 2

R

Rack Mounting 9

S

Shipping List 7
Start-up (POST) 12
Stealth Mode 26
    Address Set Allocation 28
    Configuring Multi-Switch Topologies 32
    Segmenting Private Loops 31
Support, technical 45

T

Technical Reference 42
Technical Support 45
Terms
    See Glossary
Theory of Operation 25
Troubleshooting 36
    Answers to Common Questions 40

U

Unpacking 7